02P12391

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 10 049 A 1**

(51) Int. Cl.[7]:
H 04 L 9/14
G 05 B 19/048

(21) Aktenzeichen: 101 10 049.3
(22) Anmeldetag: 2. 3. 2001
(43) Offenlegungstag: 5. 9. 2002

DE 101 10 049 A 1

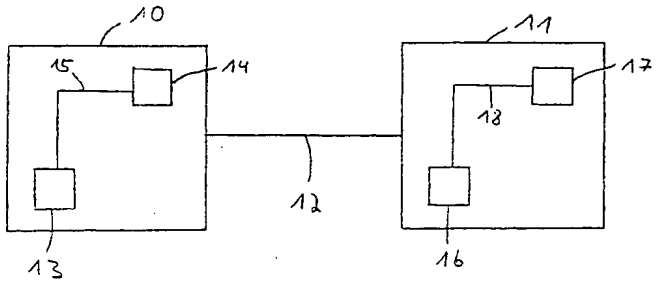
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Hurich, Martin, Dr., 71665 Vaihingen, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren und Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten

(57) Es werden ein Verfahren und eine Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten beschrieben.
Bei dem Verfahren werden die zu übertragenden Daten byteweise in einem Programmiergerät mit einem ersten Schlüssel verschlüsselt und anschließend über eine Datenleitung zu einem Steuergerät übertragen. Abschließend werden die Daten in dem Steuergerät (11) mit einem zweiten Schlüssel, der im Steuergerät (11) vorgesehen ist, entschlüsselt.



DE 101 10 049 A 1

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten.

Stand der Technik

[0002] Um zu verhindern, daß elektronisch gespeicherte Daten abgehört oder gar verändert werden, werden diese verschlüsselt. Ohne den entsprechenden Schlüssel zum Entschlüsseln können diese Daten dann nicht von einem Nichtberechtigten verwertet werden.

[0003] Bei der Programmierung von Steuergeräten wird ein Datenstrom über eine Datenleitung von einem Programmiergerät zu einem Steuergerät zu dessen Programmierung übertragen. Sowohl von Anwendern als auch vom Gesetzgeber werden mittlerweile Verfahren zur Verschlüsselung des Datenstroms gefordert. Auf diese Weise soll ein nicht bestimmungsgemäßer Zugriff auf den Inhalt der Speicherbausteine im Steuergerät verhindert werden.

[0004] Dabei ist zu beachten, dass das Verschlüsselungsverfahren geeignet sein soll, zusammen mit anderen Codierverfahren und Kompressionsverfahren verwendet zu werden, ohne an Wirksamkeit zu verlieren oder eine gegenseitige Behinderung der Verfahren zu verursachen.

[0005] Zu unterscheiden ist zwischen symmetrischen und asymmetrischen Verfahren. Bei den symmetrischen Verfahren wird ein Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln verwendet. Bei asymmetrischen Verfahren unterscheidet sich der Schlüssel zum Verschlüsseln von demjenigen zum Entschlüsseln.

[0006] Bekannt ist ein symmetrisches, blockorientiertes Verschlüsselungsverfahren, bei dem wandernde XOR-Masken zur Verschlüsselung eingesetzt werden. Dieses Verfahren zeichnet sich durch seine Einfachheit aus und eignet sich daher besonders für den Einsatz in Steuergeräten. Nachteilig ist dabei, dass größere Bereiche bekannter Daten (z. B. Füllbereiche, welche meistens aus FFh oder 00h bestehen) dem potentiellen Angreifer den Schlüssel verraten können. Besonders bei der Verwendung von Kompressionsverfahren, welche auf dem Huffmann-Coding basieren, treten üblicherweise längere Ketten gleicher Bits auf. Dies erleichtert dem Angreifer die Entschlüsselung des Codes.

[0007] Aus der US-Patentschrift 5,724,428 ist ein Verfahren zur Übertragung von Daten bekannt, welches eine Verschlüsselung und Entschlüsselung der übertragenen Daten ermöglicht. Die Druckschrift beschreibt die Verwendung eines geheimen Schlüssels, welcher wiederum in verschlüsselter Form vom Sender zum Empfänger übertragen wird. Dieser geheime Schlüssel wird im weiteren dazu verwendet, um die zu übertragenden Daten zu verschlüsseln und zu entschlüsseln.

[0008] Das Verschlüsselungsverfahren an sich verwendet ein Feld von beliebiger Größe, welches mit den zu verschlüsselnden Werten verknüpft wird. Hierbei ist von Bedeutung, dass die zu verschlüsselnden Daten zunächst in erste und zweite Worte aufgeteilt werden. Diese Worte haben beliebige, aber feste Längen. Anschließend wird auf diese Worte eine invertierbare Operation angewandt. Dabei werden zunächst die ersten Worte mit dem ersten Element des oben beschriebenen Feldes verknüpft und dann die zweiten Worte mit dem zweiten Element des Feldes verknüpft. Anschließend werden die Worte wechselweise über die invertierbare Operation miteinander verknüpft und danach um jeweils die Anzahl von Stellen rotiert, welche dem jeweils anderen Wort entspricht. Danach wird das jeweils nächste Element des oben beschriebenen Feldes zu den Worten addiert.

[0009] Da die zu verschlüsselnden Daten in erste und zweite Worte aufgeteilt werden, kann dieses Verfahren nicht auf einzelne Bytes angewendet werden. Die Tatsache, dass jedesmal der Schlüssel mit übertragen werden muss, erweist sich als aufwendig und riskant.

[0010] Die vorliegende Erfindung soll ein alternatives Verfahren und eine Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten angeben.

Vorteil der Erfindung

[0011] Das erfindungsgemäße Verfahren nach Anspruch 1 zeichnet sich dadurch aus, dass die zu übertragenden Daten zunächst in einem Programmiergerät mit einem ersten Schlüssel verschlüsselt werden, die verschlüsselten Daten über eine Datenleitung zu einem Steuergerät übertragen werden und die Daten in dem Steuergerät mit einem zweiten Schlüssel, der im Steuergerät vorgesehen ist, entschlüsselt werden.

[0012] Dadurch, dass der Schlüssel nicht mitübertragen wird, sondern bereits im Steuergerät vorgesehen ist, verringert sich die zu übertragende Datenmenge und erhöht sich die Sicherheit.

[0013] Eine erfindungsgemäße Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten weist ein Programmiergerät auf, bei dem ein erster Schlüssel vorgesehen ist, ein Steuergerät, bei dem ein zweiter Schlüssel vorgesehen ist und eine Datenleitung zur Übertragung der verschlüsselten Daten.

[0014] Vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen sowie aus der Beschreibung.

[0015] Bei dem erfindungsgemäßen Verfahren kann sowohl ein symmetrisches Verschlüsselungsverfahren als auch ein asymmetrisches Verschlüsselungsverfahren zur Anwendung kommen. Sind der erste und der zweite Schlüssel identisch, so handelt es sich um ein symmetrisches Verschlüsselungsverfahren. Sind der erste und zweite Schlüssel nicht identisch, findet ein asymmetrisches Verschlüsselungsverfahren Anwendung.

[0016] Bevorzugt wird für die Verschlüsselung eine Tabelle S mit m Elementen S_0 bis S_{m-1} verwendet. Auf diese Tabelle wird mittels einer Hash-Funktion h(x) zugegriffen. h(x) dient dabei als Index.

[0017] Ein verschlüsseltes Byte n* wird aus einem unverschlüsselten Byte n nach folgender Vorschrift gebildet (Für Entschlüsselung und Verschlüsselung ist ein Startwert n_{-1} notwendig):

$$n_i^* = \left(n_i \lll \sum_{j=0}^{i} n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^*\right)} \qquad \text{(Formel 2)}$$

[0018] Aus einem verschlüsselten Byte n* wird das unverschlüsselte Byte n nach folgender Vorschrift gebildet:

$$n_i = \left(n_i^* \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^*\right)} \right) \ggg \sum_{j=0}^{i} n_{j-1}^* \qquad \text{(Formel 3)}$$

[0019] Der Schlüssel kann sowohl als elektronischer Schaltkreis, beispielsweise in einem ASIC, implementiert sein als auch als Computerprogramm vorliegen.

[0020] Das Computerprogramm kann auf geeigneten Datenträgern, wie EEPROMs, Flash-Memories aber auch CD-ROMs, Disketten oder Festplattenlaufwerken gespeichert sein. Abgearbeitet wird das Computerprogramm von einer elektronischen Recheneinheit, zum Beispiel einem Mikroprozessor, im Programmiergerät bzw. Steuergerät.

[0021] Bevorzugt weisen das Programmiergerät und das Steuergerät jeweils eine elektronische Recheneinheit und einen Speicherbaustein auf, die über einen Datenbus miteinander verbunden sind. Als elektronische Recheneinheit dient beispielsweise ein Mikroprozessor.

[0022] Auch für denn Fall, dass der Schlüssel vom Sender zum Empfänger übertragen wird, eignet sich als Schlüssel eine Tabelle, auf die mittels einer Hash-Funktion zugegriffen wird.

Zeichnungen

[0023] Die Erfindung wird anhand der beigefügten Zeichnung näher erläutert. In dieser zeigt:

[0024] **Fig.** 1 eine bevorzugte Ausführungsform der erfindungsgemäßen Vorrichtung in schematischer Darstellung, und

[0025] **Fig.** 2 eine bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens im Flussdiagramm.

[0026] **Fig.** 1 zeigt schematisch den Aufbau einer erfindungsgemäßen Vorrichtung. Zu erkennen sind ein Programmiergerät **10**, ein Steuergerät **11** und eine Datenleitung **12**. Weiterhin sind im Programmiergerät **10** ein Mikroprozessor **13** und ein Speicherelement **14** zu erkennen, die über einen Datenbus **15** miteinander verbunden sind. Ein vergleichbarer schematischer Aufbau findet sich ebenfalls im Steuergerät **11**. In diesem sind ein Mikroprozessor **16**, ein Speicherbaustein **17** und ein Datenbus **18** dargestellt.

[0027] Nachfolgend wird die Funktionsweise der erfindungsgemäßen Vorrichtung erläutert:
Im Speicherbaustein **14** des Programmiergeräts **10** sind Daten zur Programmierung des Steuergeräts **11** abgelegt. Mittels einer Tabelle und einer Hash-Funktion, die ebenfalls im Speicherbaustein **14** gespeichert sind, werden die Daten mit dem Mikroprozessor **13** verschlüsselt.

[0028] Das Verfahren bedient sich dabei folgender reversibler Operationen:

- linksseitige Rotation (innerhalb eines Bytes): <<<
  rechtsseitige Rotation (innerhalb eines Bytes): >>>
- byteweises exklusives Oder: ⊕

[0029] Die Ergebnisse seien dabei invariant bezüglich Rotation um Vielfache von 8.

[0030] Für die Verschlüsselung wird eine Tabelle S mit m Elementen S_0 bis S_{m-1} verwendet. Auf diese Tabelle wird mittels einer Hash-Funktion h(x) zugegriffen. h(x) dient dabei als Index.

[0031] Zur einfacheren Beschreibung werden die während der Verschlüsselung aufeinanderfolgenden Bytes mit einem Index i, mit i = 0, 1, 2, . . . versehen.

[0032] Ein verschlüsseltes Byte n* wird aus einem unverschlüsselten Byte n nach folgender Vorschrift gebildet (Für Entschlüsselung und Verschlüsselung ist ein Startwert n_{-1} notwendig):

$n_{-1} \equiv S_0$ (Formel 1)

$$n_i^* = \left(n_i \lll \sum_{j=0}^{i} n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^*\right)} \qquad \text{(Formel 2)}$$

[0033] Die verschlüsselten Daten werden anschließend über die Datenleitung **12** zum Steuergerät **11** übertragen. Werden die Daten bei der Übertragung abgehört, ist dies unschädlich, da die verschlüsselten Daten ohne den Schlüssel, der nicht mit übertragen wird, nicht verwertet werden können.

[0034] Die verschlüsselten Daten werden im Speicherbaustein **17** des Steuergeräts **11** gespeichert. Im Speicherbaustein **17** befindet sich der gleiche Schlüssel wie im Speicherbaustein **14** des Programmiergerät **10**. Mit diesen werden die Daten wieder entschlüsselt.

[0035] Aus einem verschlüsselten Byte n* wird das unverschlüsselte Byte n nach folgender Vorschrift gebildet:

$$n_i = \left(n_i \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}\right)} \right) >>> \sum_{j=0}^{i} n_{j-1} \qquad \text{(Formel 3)}$$

[0036] Anschließend kann das Steuergerät **11** programmiert werden. Dabei werden die entschlüsselten Daten mit dem Mikroprozessor **16** abgearbeitet.

[0037] Das Flussdiagramm in **Fig. 2** verdeutlicht den Ablauf des erfindungsgemäßen Verfahrens.

[0038] In einem Schritt **20** wird zunächst die Verschlüsselung der Daten, welche zur Programmierung des Steuergeräts vorgesehen sind, durchgeführt. Die zu verschlüsselnden Daten werden dabei nicht, wie dies wie im Stand der Technik beschrieben ist, in erste und zweite Worte aufgeteilt. Dadurch kann das Verfahren auch auf einzelne Bytes angewendet werden. Das Verfahren wendet eine Rotation um eine Anzahl von Stellen an, welche von der gesamten Vorgeschichte der Verschlüsselung abhängig ist. Die Verschlüsselung eines Bytes ist somit nicht vorbestimmt sondern abhängig von der Vorgeschichte.

[0039] Die Elemente des Feldes werden nicht in linearer Reihenfolge eingesetzt, sondern über eine Hash-Funktion ausgewählt. Die Verknüpfung erfolgt nicht additiv, sondern über ein exklusives Oder. Ein zusätzlicher Parameter ist nicht die Anzahl der Operation, sondern die Auswahl der Hash-Funktion. Dies reduziert die Laufzeit erheblich.

[0040] In einem anschließenden Verfahrensschritt **21** erfolgt die Datenübertragung über die Datenleitung **12**. Da die übertragenen Daten verschlüsselt sind, sind sie für einen möglichen Angreifer nicht zu verwerten.

[0041] Anschließend werden in einem Verfahrensschritt **22** die Daten eingelesen, d. h. im Speicherbaustein **17** des Steuergeräts **11** abgelegt.

[0042] Abschließend erfolgt in einem Schritt **23** die Entschlüsselung der Daten. Der Schlüssel zum Entschlüsseln ist als Computerprogramm im Speicherbaustein des Steuergeräts **11** abgelegt.

[0043] Zur Entschlüsselung wird der gleiche Schlüssel wie derjenige zum Verschlüsseln verwendet. Es handelt sich somit hier um ein symmetrisches Verfahren.

[0044] Im Vergleich zum oben beschriebenen Verfahren, bei welchem wandernde XOR-Masken zur Verschlüsselung eingesetzt werden, wird der Schlüssel nicht in dem Datenstrom oder zusammen mit sonstigen Parametern übertragen, sondern befindet sich bereits im Steuergerät. Außerdem wird keine Tabelle anhand solcher Parameter aus Pseudozufallszahlen generiert.

[0045] Im Gegensatz zu bekannten Verfahren erfolgt keine Addition von Schlüsselwerten während der Ver- und Entschlüsselung. Beim erfindungsgemäßen Verfahren werden die Eingangswerte nicht auf zwei oder mehr Register zerteilt, um diese danach simultan zu verändern.

[0046] Das erfindungsgemäße Verfahren zeichnet sich dadurch aus, dass der Schlüssel, in diesem Fall die Tabelle und die Hash-Funktion, nicht im Datenstrom über die Datenleitung übertragen wird, sondern sich bereits im Steuergerät befindet.

[0047] Da das beschriebene Verfahren die Eingangswerte nicht auf zwei oder mehr Register verteilt, um diese danach simultan zu verändern, kann es auch auf einzelne Bytes angewendet werden, dies ist insbesondere im Rahmen der Anwendung innerhalb der Flashprogrammierung vorteilhaft.

[0048] Typischerweise wird das erfindungsgemäße Verfahren von einer Vielzahl von Anwendern eingesetzt werden. Deshalb muss sichergestellt sein, dass ein versehentlicher Datenaustausch zwischen verschiedenen Anwendern vermieden wird. Aufgrund der Tatsache, dass das beschriebene Verfahren parametrisierbar ist, kann dies vermieden werden.

[0049] Mit dem Verfahren sind große Bereiche mit gleichem Inhalt (Füllbereiche) sicher zu verschlüsseln. Die kodierten Bereiche geben keinen Aufschluß über den verwendeten Schlüssel. Eine byteweise Zuordnung zwischen Ein- und Ausgangsdaten ist nicht möglich.

[0050] Das Verfahren erfordert keinen temporären Speicherplatz für den Datenstrom bzw. Teile daraus. Lediglich ein Byte wird als Speicherplatz für die laufende Summe benötigt. Auch der Bedarf an Code für die Entschlüsselung ist sehr gering (ca. 130 Bytes). Für den Einsatz in Kfz-Steuergeräten ist dies von großer Bedeutung.

[0051] Es ist auch möglich, durch Verwendung einer benutzerspezifischen Tabelle das Verfahren an unterschiedliche Anforderungen anzupassen. Zusätzlich kann eine beliebige Hash-Funktion für den Tabellenzugriff verwendet werden, um mögliche Rückschlüsse auf den Inhalt der Tabelle zu erschweren.

[0052] Der Datendurchsatz bei dem beschriebenen System liegt beispielsweise bei mehr als 7 MB/Minute.

Patentansprüche

1. Verfahren zur Datenverschlüsselung bei der Programmierung von Steuergeräten (**11**), bei dem die zu übertragenden Daten in einem Programmiergerät (**10**) mit einem ersten Schlüssel verschlüsselt werden, die verschlüsselten Daten über eine Datenleitung (**12**) zu einem Steuergerät (**11**) übertragen werden und die Daten in dem Steuergerät (**11**) mit einem zweiten Schlüssel, der im Steuergerät (**11**) vorgesehen ist, entschlüsselt werden.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der erste und der zweite Schlüssel identisch sind.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der erste und der zweite Schlüssel nicht identisch sind.
4. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass als Schlüssel eine Tabelle verwendet wird, auf die mittels einer Hash-Funktion zugegriffen wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass mindestens einer der Schlüssel in einer elektronischen Schaltung implementiert ist.
6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass mindestens einer der Schlüssel als

Computerprogramm vorliegt.

7. Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten, mit einem Programmiergerät (**10**), bei dem ein erster Schlüssel vorgesehen ist, einem Steuergerät (**11**), bei dem ein zweiter Schlüssel vorgesehen ist und einer Datenleitung (**12**) zur Übertragung der verschlüsselten Daten.

8. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass der erste und der zweite Schlüssel identisch sind.

9. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass der erste und der zweite Schlüssel nicht identisch sind.

10. Vorrichtung nach einem der Ansprüche 7 bis 9, dadurch gekennzeichnet, dass das Programmiergerät und das Steuergerät jeweils eine elektronische Recheneinheit (**13**, **16**) und einen Speicherbaustein (**14**, **17**) umfassen, die über einen Datenbus (**15**, **18**) miteinander verbunden sind.

11. Computerprogramm mit Programmcode-Mitteln, um die Verschlüsselung mittels einer Tabelle und einer Hash-Funktion durchzuführen, wenn das Computerprogramm auf einer entsprechenden Recheneinheit, insbesondere in einer elektronischen Recheneinheit in einem Programmiergerät (**10**) ausgeführt wird.

12. Computerprogramm mit Programmcode-Mitteln, um die Entschlüsselung mittels einer Tabelle und einer Hash-Funktion durchzuführen, wenn das Computerprogramm auf einer entsprechenden Recheneinheit, insbesondere in einer elektronischen Recheneinheit in einem Steuergerät (**11**) ausgeführt wird.

13. Computerprogrammprodukt mit Programmcode-Mitteln, die auf einem computerlesbaren Datenträger gespeichert sind, um die Verschlüsselung mittels einer Tabelle und einer Hash-Funktion durchzuführen, wenn das Computerprogramm auf einer elektronischen Recheneinheit, insbesondere einer elektronischen Recheneinheit eines Programmiergerätes (**10**) ausgeführt wird.

14. Computerprogrammprodukt mit Programmcode-Mitteln, die auf einem computerlesbaren Datenträger gespeichert sind, um die Entschlüsselung mittels einer Tabelle und einer Hash-Funktion durchzuführen, wenn das Computerprogramm auf einer elektronischen Recheneinheit, insbesondere einer elektronischen Recheneinheit eines Steuergerätes (**11**) ausgeführt wird.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 101 10 049 A1
Int. Cl.[7]: H 04 L 9/14
Offenlegungstag: 5. September 2002

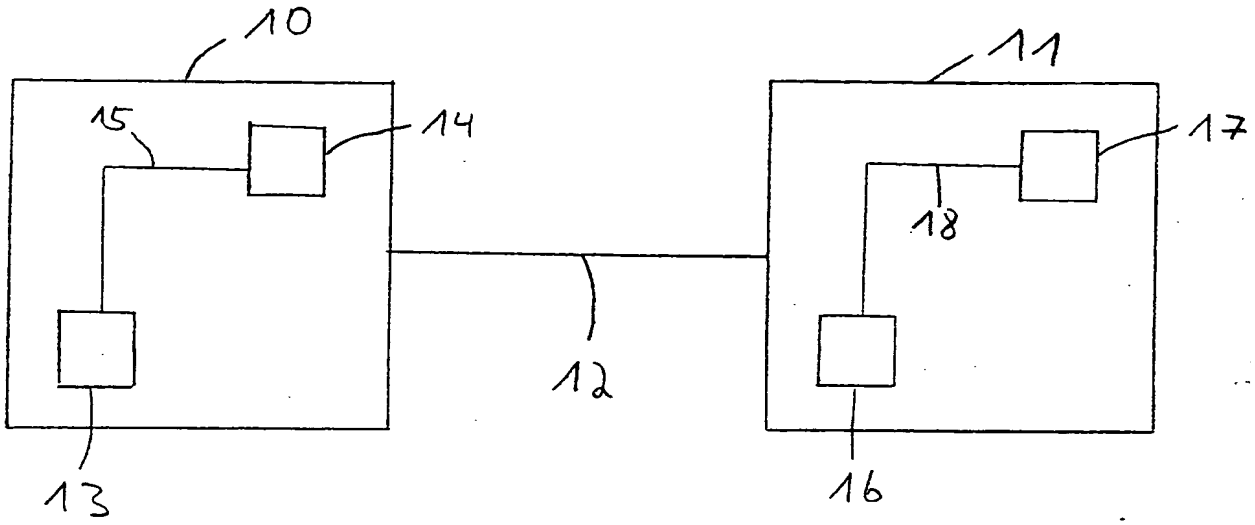


Fig. 1

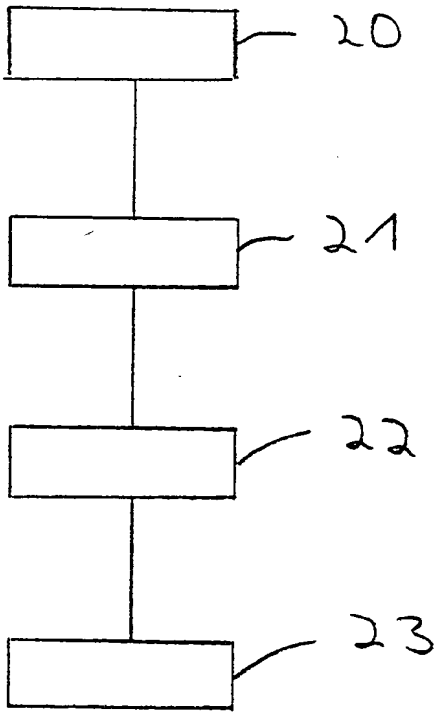


Fig. 2